EXHIBIT C-17
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 6 ('661 Patent)	**U.S. 5,165,098 to Høivik (Høivik)**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." *See also* Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Single-chip smart card processors based on these cores are made by almost all the large silicon foundries,. . . .Several marketplace forces are at work to open the smart card as a general-purpose computing platform.").
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation

message;	from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(b) a source of unpredictable information;	2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." 2:37-47 – "When the masking signal has the same or similar characteristic properties as the unintentionally radiated signal, there is obtained a good protective effect. In this connection it is an important feature that the masking comprises emission of a series of random character and letter combinations selected from a set of characters being equal to or corresponding to at least a portion of the character set which is given and is used for information processing and presentations in the data equipment concerned, and which can have the same statistical properties as the corruptive signal." 3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Claim 1 – "means (13) for selecting characters in random order from the store (14)."
(c) a processor:	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may

	be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation." Figure 1.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." Figure 1.
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during	3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:33-40 – "In order that the protective radiation 20 shall have an optimal effect, the signature of all characters which can be presented by the terminal 1 on its screen, are stored in a register, i.e. the store 14 in the form of the so-called character table I containing codes for the choice of characters concerned. The processor 13 will then read out one of these codes when a protective signal is to be emitted." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive

Exhibit C-17 (Høivik)

said processing; and	radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Figure 1.
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."

Claim 11 ('661 Patent)	**U.S. 5,165,098 to Høivik**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection

	against remote access to digital equipment which emits stray electromagnetic radiation." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation."
(c) a processor connected to said input interface for	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The

Exhibit C-17 (Høivik)

receiving and cryptographically processing said quantity; and	information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation." Figure 1.
(d) a noise production system for introducing noise into said measurement of said power consumption.	2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." 2:37-47 – "When the masking signal has the same or similar characteristic properties as the unintentionally radiated signal, there is obtained a good protective effect. In this connection it is an important feature that the masking comprises emission of a series of random character and letter combinations selected from a set of characters being equal to or corresponding to at least a portion of the character set which is given and is used for information processing and presentations in the data equipment concerned, and which can have the same statistical properties as the corruptive signal." 3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm

Exhibit C-17 (Høivik)

	which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Claim 1 – "means (13) for selecting characters in random order from the store (14)."

Claim 12 ('661 Patent)	U.S. 5,165,098 to Høivik
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." 2:37-47 – "When the masking signal has the same or similar characteristic properties as the unintentionally radiated signal, there is obtained a good protective effect. In this connection it is an important feature that the masking comprises emission of a series of random character and letter combinations selected from a set of characters being equal to or corresponding to at least a portion of the character set which is given and is used for information processing and presentations in the data equipment concerned, and which can have the same statistical properties as the corruptive signal." 3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point."

Exhibit C-17 (Høivik)

	Claim 1 – "means (13) for selecting characters in random order from the store (14)."
(b) a noise processing module for improving the random characteristic of said initial noise; and	4:25-35 – "It will be realized that if the masking signal is too weak, the effect thereof may be suppressed, which means that the masking signal must have a certain minimum strength. Further it will be realized that a stable masking signal having a constant strength or amplitude, may involve uncertainty with respect to the effect of the masking and thereby the protection. Therefore according to the invention it has been found to be an advantage to modulate the masking signal as illustrated in FIG. 3. The superimposed amplitude modulation gives a further improved protection by the system."
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	4:25-35 – "It will be realized that if the masking signal is too weak, the effect thereof may be suppressed, which means that the masking signal must have a certain minimum strength. Further it will be realized that a stable masking signal having a constant strength or amplitude, may involve uncertainty with respect to the effect of the masking and thereby the protection. Therefore according to the invention it has been found to be an advantage to modulate the masking signal as illustrated in FIG. 3. The superimposed amplitude modulation gives a further improved protection by the system."

Claim 26 ('661 Patent)	**U.S. 5,165,098 to Høivik**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying

Exhibit C-17 (Høivik)

	and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(b) generating unpredictable information;	2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." 2:37-47 – "When the masking signal has the same or similar characteristic properties as the unintentionally radiated signal, there is obtained a good protective effect. In this connection it is an important feature that the masking comprises emission of a series of random character and letter combinations selected from a set of characters being equal to or corresponding to at least a portion of the character set which is given and is used for information processing and presentations in the data equipment concerned, and which can have the same statistical properties as the corruptive signal." 3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:41-53 – "The most important property of the protective signal, in addition to being analogous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely

Exhibit C-17 (Høivik)

	random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Claim 1 – "means (13) for selecting characters in random order from the store (14)."
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:33-40 – "In order that the protective radiation 20 shall have an optimal effect, the signature of all characters which can be presented by the terminal 1 on its screen, are stored in a register, i.e. the store 14 in the form of the so-called character table I containing codes for the choice of characters concerned. The processor 13 will then read out one of these codes when a protective signal is to be emitted." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Figure 1.

by selecting a code process from a plurality of code processes, where said selected code process is involved in said cryptographic processing,	3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:33-40 – "In order that the protective radiation 20 shall have an optimal effect, the signature of all characters which can be presented by the terminal 1 on its screen, are stored in a register, i.e. the store 14 in the form of the so-called character table I containing codes for the choice of characters concerned. The processor 13 will then read out one of these codes when a protective signal is to be emitted." Claim 1 – "means (13) for selecting characters in random order from the store (14)."
but where the value of said outputted quantity is independent of which of said code processes was selected; and	3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:33-40 – "In order that the protective radiation 20 shall have an optimal effect, the signature of all characters which can be presented by the terminal 1 on its screen, are stored in a register, i.e. the store 14 in the form of the so-called character table I containing codes for the choice of characters concerned. The processor 13 will then read out one of these codes when a protective signal is to be emitted." Claim 1 – "means (13) for selecting characters in random order from the store (14)."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the

Exhibit C-17 (Høivik)

	information."

Claim 29 ('661 Patent)	U.S. 5,165,098 to Høivik
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 2:14-22 – "An object of the present invention is to obtain protection which can be provided comparatively easily in connection with existing data equipment at the same time as it can be integrated in a relatively simple and inexpensive manner into new equipment being produced. Moreover it is an object of the invention to provide a system which in a better and more flexible way affords protection against remote access to digital equipment which emits stray electromagnetic radiation."
(b) receiving a	1:5-11 – "Data security is today in focus at the same time as EDP is

Exhibit C-17 (Høivik)

quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." 2:37-47 – "When the masking signal has the same or similar characteristic properties as the unintentionally radiated signal, there is obtained a good protective effect. In this connection it is an important feature that the masking comprises emission of a series of random character and letter combinations selected from a set of characters being equal to or corresponding to at least a portion of the character set which is given and is used for information processing and presentations in the data equipment concerned, and which can have the same statistical properties as the corruptive signal." 3:28-32 – "The protection module is built up around the micro-processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the

	same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Claim 1 – "means (13) for selecting characters in random order from the store (14)."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:5-11 – "Data security is today in focus at the same time as EDP is being increasingly introduced into new fields of use. Often there may be large amounts of information collected in a single system. The information contained in an electronic data processing plant is usually protected by conventional methods such as security zones, code words and restricted access." 1:12-15 – "A potential source of leakage which has not attracted much attention, apart from defence applications, is electromagnetic radiation from peripheral equipment, for example terminals and printers." 2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information."

Claim 30 ('661 Patent)	U.S. 5,165,098 to Høivik
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	2:30-36 – "In short this invention provides for the masking of corruptive radiation from computer equipment by emitting a coded masking signal which together with the actual information-carrying and corruptive signal will form a modified corruptive signal which to a high degree makes it difficult to detect or remotely access the information." 2:37-47 – "When the masking signal has the same or similar characteristic properties as the unintentionally radiated signal, there is obtained a good protective effect. In this connection it is an important feature that the masking comprises emission of a series of random character and letter combinations selected from a set of characters being equal to or corresponding to at least a portion of the character set which is given and is used for information processing and presentations in the data equipment concerned, and which can have the same statistical properties as the corruptive signal." 3:28-32 – "The protection module is built up around the micro-

	processor 13 which quite at random selects which character the protective signal shall represent, modulates the signal and administrates the emission of the protective radiation 20." 3:41-53 – "The most important property of the protective signal, in addition to being analagous or identical in nature to the corruptive radiation, is that the characters emitted are selected in a completely random order or have a statistical distribution of characters corresponding to the radiated signal. This is obtained thereby that the micro-processor 13 in its programme table has stored an algorithm which generates a random sequence, which can take place in a manner which is known per se. If it is desired to avoid the repetition of the same sequence each time the equipment is started up, there can be utilized a circuit for generating a statistically random starting point." Claim 1 – "means (13) for selecting characters in random order from the store (14)."
(b) improving the random characteristic of said initial noise; and	4:25-35 – "It will be realized that if the masking signal is too weak, the effect thereof may be suppressed, which means that the masking signal must have a certain minimum strength. Further it will be realized that a stable masking signal having a constant strength or amplitude, may involve uncertainty with respect to the effect of the masking and thereby the protection. Therefore according to the invention it has been found to be an advantage to modulate the masking signal as illustrated in FIG. 3. The superimposed amplitude modulation gives a further improved protection by the system."
(c) varying said power consumption based on said improved initial noise.	4:25-35 – "It will be realized that if the masking signal is too weak, the effect thereof may be suppressed, which means that the masking signal must have a certain minimum strength. Further it will be realized that a stable masking signal having a constant strength or amplitude, may involve uncertainty with respect to the effect of the masking and thereby the protection. Therefore according to the invention it has been found to be an advantage to modulate the masking signal as illustrated in FIG. 3. The superimposed amplitude modulation gives a further improved protection by the system."